ABSTRACT

A method for protecting a portable card, provided with at least a crypto algorithm for enciphering data and/or authenticating the card, against deriving the secret key through statistical analysis of its information leaking away to the outside world in the event of cryptographic operations, such as power-consumption data, electromagnetic radiation and the like. The card is provided with at least a shift register having a linear and a non-linear feedback function for creating cryptographic algorithms. An algorithm is applied to the card, which is constructed in such a manner that the collection of values of recorded leak-information signals is resistant to deriving the secret key from statistical analysis of those values. Advantageously, after the key has been loaded into the shift register, the shift register clocks on, using at least the linear-feedback function. A suitable alternative is loading only the key into the shift register in the event of a fixed content of the shift register.